Communications Security Establishment Commissioner

The Honourable Jean-Pierre Plouffe, CD

Commissaire du Centre de la sécurité des télécommunications

L'honorable Jean-Pierre Plouffe, CD

January 30, 2018

The Honourable John McKay, MP
Chair
Standing Committee on Public Safety and National Security
House of Commons
6th Floor, 131 Queen Street
Ottawa, Ontario K1A 0A6

Dear Mr. McKay:

In the context of Bill C-59, *An Act respecting national security matters*, having been referred to committee before Second Reading, I am writing to provide you with additional proposals respecting Part 2 of the Bill, the *Intelligence Commissioner Act* and Part 3, the *Communications Security Establishment Act,* that I provided to Ministers Goodale and Sajjan in November. Given the quasi-judicial function of the Intelligence Commissioner (IC), the requirement that the IC be a retired judge of a Superior Court, and given the transition clause in the IC Act, I am directly implicated in these proposed Acts.

Le 30 janvier 2018

L'honorable John McKay, député
Président
Comité permanent de la sécurité publique et nationale
Chambre des communes
131, rue Queen, 6e étage
Ottawa (Ontario) K1A 0A6

Monsieur McKay,

Étant donné que le projet de loi C-59, *Loi concernant des questions de sécurité nationale*, a été renvoyé au comité responsable avant la deuxième lecture, je vous écris pour vous présenter des propositions supplémentaires concernant la partie 2 du projet de loi, la *Loi sur le commissaire au renseignement*, et la partie 3, la *Loi sur le Centre de la sécurité des télécommunications,* que j'ai envoyées aux ministres Goodale et Sajjan au mois de novembre. Compte tenu de la fonction quasi judiciaire du commissaire au renseignement, de l'exigence selon laquelle le commissaire au renseignement doit être un juge à la retraite d'une juridiction supérieure et de la clause transitoire prévue dans la *Loi sur le commissaire au renseignement*, je suis directement touché par ces lois proposées.

The Honourable/l'honorable Jean-Pierre Plouffe, CD

P.O. Box/C.P. 1474, Station "B" / Succursale «B»
Ottawa, Ontario K1P 5P6
Tel: 613-992-3044, Fax: 613-992-4096
info@ocsec-bccst.gc.ca

Substantive Proposals Regarding the Intelligence Commissioner's Role

Proposal 1

The Intelligence Commissioner (IC) should approve the active cyber operations in addition to the defensive cyber operations that are authorized by the Minister[1] pursuant to subsections 30(1) and 31(1) of the *Communications Security Establishment Act* (CSE Act).

Discussion

Active Cyber Operations

Although the IC must approve foreign intelligence authorizations and cybersecurity authorizations issued by the Minister, the IC has no role when it comes to the issuance by the same Minister of active or defensive cyber operations authorizations. The reason, we understand, is that these authorizations do not involve the collection of information and hence privacy interests are reduced or eliminated.

The new mandate of the Communications Security Establishment (CSE) for active cyber operations is found at section 20 of the proposed CSE Act. In accordance with this section, CSE will carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.

The Chief of CSE must make a written application and set out the facts that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary, and that the conditions to issue it are met. Also, the Minister of Foreign Affairs would need to either consent or be the one requesting the active cyber operation in order for the authorization to take place.

These active cyber activities, similar to the ones provided for in the *Canadian Security Intelligence Act* (CSIS Act) with respect to disrupting a communication or means of communications, can take place not only with respect to security matters (i.e. the Canadian Security Intelligence Service [CSIS] can only undertake threat reduction activities when it concerns a threat to the security of Canada), but also for international affairs and defence matters. In essence, CSE could ask the Minister to authorize active cyber activities on a matter that would be purely of an international affairs nature, such as communications surrounding an international gathering on the economy or the environment. Indeed, this would meet the requirement of being about the intentions or capabilities of a foreign state with respect to an international affairs matter. Currently, there is no role envisaged for the IC to approve such an authorization, even where third party rights, including their privacy rights, and freedoms could

[1] The Intelligence Commissioner is to review authorizations/determinations of either a Minister or the Director of the Canadian Security Intelligence Service. For convenience, the term "Minister" will be used throughout this document.

be affected, including those of a Canadian outside of Canada, or where a Canadian law could be contravened.

Indeed, when considering this new mandate, the Department of Justice, in a document entitled *Charter Statement – Bill C-59: An Act respecting national security matters*[2], stated the following:

> The provisions authorizing active cyber operations would not by definition engage any Charter rights or freedoms. However, specific activities authorized under this scheme could potentially engage rights or freedoms. The considerations that support the consistency of this aspect of the mandate with the Charter are very similar to those supporting the consistency of the defensive cyber operations mandate.

In contrast, in order for a threat disruption activity to take place under the CSIS Act, within or outside Canada, the Director of CSIS must not only get the approval of the Minister but also present the matter before a Federal Court judge and obtain a warrant where a right or a freedom under the Charter would be limited by way of the measure, or if the measure would otherwise be contrary to Canadian law. Bill C-59 is proposing to amend the CSIS Act to add at paragraph 21.1(2)(c) that for the threat reduction measure to be reasonable and proportional, consideration must be given to the reasonably foreseeable effects on third parties, including on their rights to privacy.

A comparison between the current and proposed CSIS processes with the proposed CSE processes for these activities reveals the following:

- Both CSE and CSIS may disrupt communications and means of communications.

- The nature and types of measures described in the CSIS Act and the CSE Act are similar. For example, proposed paragraph 21.1(1.1)(a) of the CSIS Act states that CSIS may *alter, remove, replace, destroy, disrupt or degrade a communication or means of communication* while the proposed active cyber mandate described in section 20 of the CSE Act states that CSE can *degrade, disrupt, influence, respond to or interfere* with the capabilities, intentions, or activities of foreign entities and the active cyber operation activities the Minister may authorize in the proposed section 32 of the CSE Act include *installing, maintaining, copying, distributing, searching, modifying, disrupting, deleting or intercepting anything on or through the global information infrastructure.*

- Both CSE and CSIS conduct these activities outside of Canada (CSIS can also conduct them within Canada).

- Neither CSE nor CSIS collect information when undertaking these activities.

---

[2] http://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/ns-sn.html, p. 9.

- CSIS threat reduction activities are limited to those measures that will reduce threats to the security of Canada while CSE's active cyber operations are broader, as they may relate not only to security, but also to international affairs or defence.

- Warrants issued by the Federal Court authorizing CSIS to take measures to reduce threats to the security of Canada are valid up to 120 days; under the proposed CSE regime, an authorization can be valid for up to one year.

- Under the CSIS Act, the Director of CSIS, the responsible Minister and the Federal Court must approve these activities in certain situations; under the CSE Act, only the Chief of CSE, the responsible Minister and the Minister of Foreign Affairs are involved in the decision-making process. However, **no independent oversight body** approves this decision under the CSE Act, even in situations where *Charter* rights or privacy rights of third parties (including those of an incidentally affected Canadian) would be engaged or a Canadian law could be contravened.

In addition, as stated earlier, the IC will be mandated to approve foreign intelligence authorizations. Analysis of subsection 27(2) of the CSE Act, which provides that the Minister may authorize listed activities in a foreign intelligence context, specifies at paragraph (c) that CSE may conduct the following activities: *"installing, maintaining, copying, distributing, searching, modifying, disrupting, deleting or intercepting anything on or through the global information infrastructure"*. This is the same list of activities to be authorized for active cyber operation appearing in section 32 of the CSE Act. Furthermore, it is unlikely that CSE would conduct active cyber operations without having a foreign intelligence ministerial authorization in place. Given that the IC will be asked to approve the same activities in a foreign intelligence context and that active cyber operations will likely not be conducted without the benefit of a foreign intelligence ministerial authorization, the IC should also approve active cyber operations authorizations.

Defensive Cyber Operations

The discussion above also generally applies to Defensive Cyber Operations. Although CSE's defensive and active cyber operations mandates differ, (see sections 19 and 20 of the CSE Act), the means to attain those goals are similar. Indeed, sections 32 and 33 of the CSE Act provide for the same activities to be authorized (for example "*installing, maintaining, copying, distributing, searching, modifying, disrupting, deleting or intercepting anything on or through the global information infrastructure*"), and provide for the same prohibitions for both active and defensive cyber operations.

Therefore, the same potential effects on third party privacy rights and freedoms and contravention of Canadian law could occur whether an active or defensive cyber operation is contemplated. Furthermore, since CSE will likely conduct defensive cyber operations in conjunction with cybersecurity ministerial authorizations (to allow for the collection of information), the latter which are also approved by the IC, it follows that the IC should also review defensive cyber operations authorizations.

Approval of Active and Defensive Cyber Operations by the IC

The rationale for having the IC involved in the decision-making authority for both active and defensive cyber operations include the following:

- It would bring consistency to the CSIS and CSE models for similar types of activities that could involve privacy rights or contravention of a Canadian law.

- Since the conditions for authorization to be assessed by the Minister in reaching a decision consist of legal criteria of a judicial nature, it is suggested that the inclusion of a quasi-judicial process in these matters would be beneficial.

- The serious nature of these matters, their complexity and their potential impact and effects on, *inter alia*, privacy rights of third parties call for the inclusion of a quasi-judicial process.

Additionally, for active cyber operations:

- The proposed CSE active cyber operations can potentially have a wider impact as they are not limited to security matters as are the CSIS threat reduction measures.

Finally, from an academic perspective, both Professor Craig Forcese, and blogger Bill Robinson, commented on the absence of a role for the IC in the context of these new active and defensive cyber operations. Professor Forcese said about Bill C-59 that "*[...] here are some curious omissions*". A paragraph later, he indicates "*[...] while the Commissioner will be busy overseeing information collected during CSE's intelligence and classic "cybersecurity" functions, we note he or she appears to have no oversight role in relation to active (and the related "defensive") cyber operations.*" Finally, he concludes "*Overall, the limits on active CSE cyber conduct seem too permissive.*"

Blogger Bill Robinson said "*[...] to my mind addition of a cyber operations mandate is a huge change in the nature of the agency, and it raises a number of issues.*" On the role of the IC, he simply underlined: "*Note, however, that a proposed new category of authorizations pertaining to offensive and defensive cyber operations, i.e. Computer Network Attack activities, would not be subject to this procedure, or indeed examined by the Intelligence Commissioner at all.*"

Proposal 2

The IC should have the right to *request clarifications* with respect to the information presented to him, short of receiving or accessing information that the Minister would not have seen.

Discussion

As currently worded, section 23 of the IC Act does not permit the IC to seek clarification from the Minister or from the requesting agency when the IC is reviewing a Minister's decision. In situations where clarification would be needed, but impossible to obtain, the IC would have no

choice but to refuse to approve the Minister's decision. It is proposed that, short of asking for additional information and ensuring that no new information would be provided to him, the IC be entitled to make requests aimed at clarifying the information that was before the Minister. This would add a degree of flexibility to the process with the goal of making it more efficient.

Additionally, it has been proposed that a review based on reasonableness might not be sufficient for purposes of *Charter* compliance given that: the IC cannot challenge the record that was before the Minister; the IC cannot benefit from representations; nor can the IC seek clarification. However, adding the possibility of seeking clarifications would make it more Charter compliant.

Proposal 3

The IC should be able to *conditionally* approve authorizations, pursuant to section 13 of the IC Act.

Discussion

There will be circumstances where the IC will have no choice but to deny an authorization based on lack of reasonableness. However, this could be avoided in certain circumstances, if the IC could conditionally approve authorizations. The insertion of a condition could enable the IC to reach a different conclusion. The scheme could provide that the IC may send the matter back to the Minister for the said condition to become part of the authorization. In practice, the IC would be issuing a conditional approval that would become valid once the condition would have been added to the initial authorization by the Minister. This would add a degree of flexibility to the process with the goal of making it more efficient.

Proposal 4

The IC should prepare a public annual report to the Prime Minister for him to table in both Houses.

Discussion

The IC is independent of government and will undertake a quasi-judicial role. Public reporting helps demonstrate this independence and will enhance transparency, accountability and, by the same token, public trust. We propose following a model like the one the United States Foreign Intelligence Surveillance Court has developed for its annual report, consisting mainly of statistics on, for example, the number of applications made and the orders granted, modified or denied. If an annual report was to be produced, the number of cases where a decision was rendered with reasons could be made public, as well as an unclassified version of those reasons.

Proposal 5

Subsection 21(1) of the IC Act should provide that while the decision of the IC must be made within a 30-day period, the reasons could follow later.

Discussion

As is the case for a judicial judgment, the notion of "reasons to follow" should apply to the IC's decisions. This would ensure that the decision is released within its statutory deadline while allowing the IC the required time, if necessary, to write detailed and clear reasons, for the benefit of the Minister and the agencies. The legislation could specify that there can be a delay for the reasons to be released. Such a delay could apply in all cases, whether the IC's decision is positive or negative.

Proposal 6

Regarding subsection 37(3) of the CSE Act, it is suggested that the decision by a Minister to extend, for one more year, an authorization on matters of foreign intelligence or cybersecurity should be reviewable by the IC.

Discussion

We believe that if the IC was involved in the initial authorization, he should be playing the same role a year later. The Minister will undoubtedly be presented with evidence to support the need for an extension. If that is the case, and the Minister reaches the conclusion to extend the authorization period, then the IC should approve this decision. If the intent of the section is for the Minister to automatically grant the extension, then it is possible that in practice these authorizations will have a two-year validity period.

Proposal 7

Paragraph 273.65(2)(c) of the *National Defence Act*, which imposes the following condition, states that the Minister needs to be satisfied that "the expected foreign intelligence value of the information that would be derived from the interception justifies it". This has not been replicated in Bill C-59 and should be added.

Discussion

We believe that this condition should be inserted in section 35 of the CSE Act. From a review and approval perspective, it would enable the IC to consider this factor in his reasonableness test.

Proposal 8

Sections 38 to 40 of the CSE Act provide for a regime dealing with "repeal and amendment" that appears inconsistent and should be re-examined.

Discussion

The proposed regime suggests that when there is a "significant change in any fact that was set out in the application for an authorization issued under subsection 27(1), 28(1) or (2), 30(1) or 31(1)", the Minister can either repeal the authorization or amend it. It is difficult to contemplate that an authorization could be amended rather than repealed after it has been determined that there is a *significant change* in a fact that led to an authorization. If there is such a change of importance and of consequence that affects CSE's activities and the Minister's decision, a new ministerial authorization should be issued, not simply amended.

Proposal 9

Subsection 41(2) of the CSE Act should provide that emergency authorizations issued by the Minister in foreign intelligence and cybersecurity matters are reviewable by the IC and base its process on the United Kingdom model under the *Investigatory Powers Act 2016*.

Discussion

Subsection 41(2) of the CSE Act currently provides that emergency authorizations issued by the Minister in foreign intelligence (subsection 27(1) of the CSE Act) and cybersecurity (subsections 28(1) and (2) of the CSE Act) matters are not reviewable by the IC. These authorizations are valid for a period of 5 days (section 43 of the CSE Act).

Section 11.22 of the CSIS Act provides that the Director of CSIS may authorize the query of a dataset that has not been retained by court order (Canadian dataset) or by decision of the Minister (foreign dataset). The Director may authorize this query only where **exigent circumstances** are present. Nevertheless, the section provides **that the IC must approve the authorization** of the Director in order for it to be valid (section 11.23 of the CSIS Act). So although the decision will be made in instances where urgency is clearly present, the law provides that the IC should play a role of reviewer.

In addition, under the *Investigatory Powers Act 2016* (IP Act), there is a very similar if not identical scheme as the one proposed in sections 41 to 43 of the CSE Act dealing with emergency authorizations.

109 Approval of warrants issued in urgent cases

(1) This section applies where—
(a) a warrant under this Part is issued ***without the approval of a Judicial Commissioner****, and*
(b) the person who issued the warrant considered that there was an urgent need to issue it.

(2) The person who issued the warrant ***must inform a Judicial Commissioner that it has been issued.***

(3) The ***Judicial Commissioner must****, before the end of the relevant period—*
(a) ***decide whether to approve the decision to issue the warrant****, and*

(b) notify the person of the Judicial Commissioner's decision.
"The relevant period" means the period ending with the third working day after the day on which the warrant was issued.

(4) ***If a Judicial Commissioner refuses to approve*** *the decision to issue a warrant, the warrant—*
(a) ***ceases to have effect*** *(unless already cancelled), and*
(b) may not be renewed,
and section 108(5) does not apply in relation to the refusal to approve the decision.
(emphasis added)

Section 116 of the IP Act provides that urgent warrants are also valid for a period of 5 days, similar to section 43 of the CSE Act.

Proposals for Technical Amendments to the *Intelligence Commissioner Act*, the *Communications Security Establishment Act* and the *Canadian Security Intelligence Service Act*

Proposal 1

The wording in subsection 23(1) of the *Intelligence Commissioner Act* (IC Act) should be clarified to specify what is included in "all information that was before [the Minister[1]]" that is provided to the Intelligence Commissioner (IC).

Discussion

Subsection 23(1) of the IC Act currently states that the IC is to be provided with "all information that was before the person who issued or amended the authorization or made the determination at issue". Since the person whose conclusions are being reviewed by the IC will likely not be presented with only written materials, it is proposed that the subsection be modified to add that the information to be provided to the IC includes, for example, any verbal exchanges, briefing notes or preparation material that the Minister was privy to.

This detailed information could be inserted in regulation. The regulation could also state that the Minister attest that the information provided to the IC for review constitutes the whole record.

Proposal 2

Regulation-making authority should be inserted in the IC Act to enable the creation of regulations for carrying out the purposes and provisions of the Act, as well as on more specific matters.

Discussion

Regulation-making authority would, for instance, allow the government and the IC to agree on the approval process/procedure of the IC in his dealings with the Ministers. It could also provide clarity for what is meant by "all information" in subsection 23(1) of the IC Act, e.g. that it includes any verbal communications or briefing materials. Section 61 of the CSE Act could be used as a model for this type of clause.

Proposal 3

The *Communications Security Establishment Act* (CSE Act) and the *Canadian Security Intelligence Service Act* (CSIS Act) should clearly provide that both the authorization/determination and all information that led to the decision by the Minister should be provided to the IC for the purpose of his review.

---

[1] The Intelligence Commissioner is to review authorizations/determinations of either Ministers or the Director of the Canadian Security Intelligence Service. For convenience, the term "Minister" will be used throughout this document.

Discussion

Section 49 of the CSE Act should be aligned with subsection 23(1) of the *IC Act* to provide that the IC should receive not only the authorization but "all information that was before the person who issued or amended the authorization or made the determination at issue". Currently, section 49 states that the 30-day time limit for the IC to provide a decision starts when the IC receives the authorization. However, there is no mention in that section that he should also receive all information that supported the authorization. Without that information, no review is possible by the IC. This should also be referenced in the CSIS Act.

Proposal 4

The wording in section 13 of the IC Act should be amended to state that the IC should review all the *information* in order to determine whether the *conclusions* of the Minister are reasonable.

Discussion

Currently, section 13 of the IC Act reads as follows:

Review and approval

13 The Commissioner is responsible, as set out in sections 14 to 21, for

> **(a)** reviewing the conclusions on the basis of which certain authorizations are issued or amended, and certain determinations are made, under the *Communications Security Establishment Act* and the *Canadian Security Intelligence Service Act*; and
>
> **(b)** if those conclusions are reasonable, approving those authorizations, amendments and determinations.

It is suggested that the section be modified to add the following:

13 The Commissioner is responsible, as set out in sections 14 to 21, for

> **(a)** reviewing **all information** on the basis of which certain authorizations are issued or amended, and certain determinations are made, under the *Communications Security Establishment Act* and the *Canadian Security Intelligence Service Act*; and
>
> **(b)** if **the conclusions of that matter** are reasonable, approving those authorizations, amendments and determinations. (emphasis added)

This modification is suggested because, in practice, the IC is reviewing all the information that leads to a decision, not only the conclusions. After reviewing all the information, the IC will be in a position to determine if the conclusions are reasonable under subsection 13(b).

Proposal 5

Section 25 of the IC Act should clarify the type and nature of the information being contemplated, such as briefings, or backgrounders, to help the IC exercise his role. The word "may" should be replaced by "must" for information requested by the IC.

Discussion

Section 25 of the IC Act currently reads as follows:

Disclosure of information to Commissioner

25 Despite any other Act of Parliament and subject to section 26, the following persons or bodies **may** — for the purpose of assisting the Commissioner in the exercise of his or her powers and the performance of his or her duties and functions — disclose to the Commissioner any information that is not directly related to a specific review under any of sections 14 to 20:

(a) the Minister of Public Safety and Emergency Preparedness;
(b) the *Minister*, as defined in section 2 of the *Communications Security Establishment Act*;
(c) the Canadian Security Intelligence Service; and
(d) the Communications Security Establishment. (emphasis added)

Section 25 is crucial to the mandate of the IC as it will enable him to be briefed and educated on matters of interest by way of technical briefings and demonstrations, expert briefings and training. It is clear that section 25 does not relate to a specific review. We note that the ability to disclose information to the IC is discretionary, as specified by the use of the word "may" in the section. However, we suggest adding that the persons or bodies "must" provide the information when requested by the IC. In essence, the agencies will be able to "push" information to the IC on a voluntary basis but the IC will be able to authoritatively "pull" necessary information from the agencies by formally requesting it.

Proposal 6

The IC Act should provide that records obtained by the IC in the course of his duties are not under the IC's control, for *Access to Information Act* and *Privacy Act* purposes.

Discussion

This essentially mirrors sections 58 and 59 of the CSE Act which state that principle. It will allow the IC to send such requests to those who will have provided him with that information. It should not be up to the IC to decide what should be publicly released or not because he is not the producer of that information.

Proposal 7

The wording in subsection 11.03(3) of the CSIS Act should be similar to that in subsections 29(1) of the CSE Act and section 11.23 of the CSIS Act.

Discussion

In order to be consistent with other parts of Bill C-59, it is suggested that wording such as "the determination is valid when approved by the IC", or something similar, be added to section 11.03 of the CSIS Act. As currently worded, subsection 11.03(3) of the CSIS Act indicates that the Minister is to notify the IC of the Minister's determination for the purpose of the IC's review and approval under the IC Act. However, it does not specify that the determination becomes valid only once approved by the IC.

Proposal 8

Some terms found in Bill C-59 should be defined or clarified for the benefit of those responsible for enforcing the legislation, as well as those who will be asked to issue authorizations or approvals.

Discussion

After reviewing Bill C-59, we believe the following terms would benefit from definition or clarification:

a. "information" (as used throughout the CSE Act);
b. "acquire", "collection" and "interception" (as used in the CSE Act, as well as the CSIS Act; the term "interception" is defined in the *Criminal Code* but is problematic with respect to the foreign intelligence collection process);
c. "disclosure" and "disseminate" (as used in the CSE Act);
d. "predominantly" (as used in the CSIS Act);
e. "publicly available dataset" (this term is defined in the CSIS Act but the definition is circular);

Proposal 9

The entity proposed as the IC should be called the "*Judicial Intelligence Commissioner*" or the "*Judicial Commissioner for Intelligence*" and the title of the legislation changed to reflect the name.

Discussion

The current proposed name does not reflect the quasi-judicial role that the IC will be asked to play. The proposed names would not only clearly signal the judicial aspect of the function but also underscore the notion of the independence of the Commissioner. This would help the public

and Parliamentarians better understand the role of the IC. It would also follow the approach taken by both the United Kingdom and New Zealand.

Proposal 10

The threshold set out in subsection 11.03(2) of the CSIS Act, is too low and will make the IC's review practically impossible.

Discussion

Currently, subsection 11.03(2) of the CSIS Act states:

Criteria

11.03(2) The Minister may determine that a class of Canadian datasets is authorized to be collected if the Minister concludes that the querying or exploitation of any dataset in the class **could lead to results that are relevant to the performance of the Service's duties and functions set out under sections 12, 12.1 and 16.** (emphasis added)

We believe that there are not that many instances were one would be able to conclude that a class of datasets could not lead to results that are relevant. To avoid making the IC's role simply that of a "rubber stamp", we suggest using the higher threshold of "is likely to assist". This standard is used by the Federal Court to determine if data should be retained as described in section 11.17 of the *CSIS Act*.

Proposal 11

The Minister responsible for the IC Act should be the Prime Minister.

Discussion

Section 3 of the IC Act provides that the Governor in Council may designate a minister as the Minister responsible for this Act. Both the Minister of National Defence and the Minister of Public Safety will have authorizations or determinations reviewed and approved by the IC and having either of them designated could possibly put them in a conflict of interest, if not give the appearance of a conflict. In addition, the Prime Minister is the one who recommends who should be appointed as the IC. We believe that the Prime Minister should be the Minister responsible for this Act.

Proposal 12

The period of validity for authorizations issued under subsections 30(1) and 31(1) of the CSE Act should be up to 6 months.

Discussion

The CSIS Act provides a period of validity of 3 months for threat reduction authorizations involving communications or means of communications while regimes in both Australia and the United Kingdom provide for a 6-month period. Currently, such an authorization under section 37(1) of the CSE Act says that it could be valid for up to one year, which we believe is too long.

Proposal 13

Section 10 of the IC Act should clarify that the concept of legal advisor is covered by the term "person having specialized knowledge".

Discussion

Subsection 273.63(5) of the *National Defence Act* currently provides that the Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties. However, section 10 of the IC Act does not specifically state that the Commissioner may engage the services of legal counsel. In order to ensure that the IC can engage legal counsel, and bearing in mind the quasi-judicial role of the IC, it should be provided for specifically.